COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNet)

PUBLICATION 1
ANNEX C

CFBLNET SECURITY AND INFORMATION ASSURANCE STRATEGY

Version 6.0
October 2009

DOCUMENT CONTROL AND TRACKING METADATA

Security Classification	Unclassified
Access Status	Version 6.0
Usage Condition	Publicly Releasable

Scheme Type	CFBLNet Documentation Control and Tracking Scheme
Scheme Name	See Pub 1, Annex G, CFBLNet Document Management
Title Words	CFBLNet Pub 1 – Annex C, CFBLNet Security and Information Assurance Strategy

Function Descriptor	Security and Information Assurance Strategy
Activity Descriptor	Implementation and Guidance

Event Date	**Agent Type**	**Agent Name**	**Agent Details**	**Event Type**	**Event Description**
30Oct09	C-EG	Steve Pitcher	C-EG Chair	Review/Approve Sign	Publication 1, Version 6.0

TABLE OF CONTENTS

APPENDICES

APPENDIX 1 – CFBLNET RISK ENVIRONMENT AND MITIGATION STRATEGY

APPENDIX 2 – CFBLNET SITE INTERCONNECTION APPROVAL GUIDELINES

APPENDIX 3 – CFBLNET INITIATIVE CONNECTION APPROVAL GUIDELINES

APPENDIX 4 – MSAB ACCREDITATION ENDORSEMENT PROCESS

APPENDIX 5 – MSAB NATIONAL ACCREDITATION ENDORSEMENT CERTIFICATE (NAEC) TEMPLATE

APPENDIX 6 – CLASSIFICATION GUIDANCE FOR THE CFBLNET

Note: All Annex C Appendices are contained in a separate document

CHAPTER 1 – INTRODUCTION

Purpose

101. Annex C to the CFBLNet Pub 1 contains the security management policies, processes and procedures, related to the execution of Initiatives on the CFBLNet, which functions under the authority of the CFBLNet Technical Arrangement (Charter).

102. In particular, Annex C provides the following information to CFBLNet users:

a. Background information to provide a broader understanding of the threats and vulnerabilities of the CFBLNet (Appendix 1).
b. Information for the secure connection of national/organization sites to the CFBLNet backbone (Appendix 2).
c. Guidance for the secure connection and operation of CFBLNet Initiatives (Appendices 3).
d. The process for certification and accreditation of CFBLNet sites and Initiatives.

103. Any Initiative using directly or indirectly the CFBLNet infrastructure shall comply with all the security regulations as laid down in Annex C.

Authority

104. Annex C is issued by the CFBLNet Executive Group (C-EG) on behalf of the C-SSG. The provisions of this and associated Publications shall govern the conduct of all business performed by the CFBLNet Participants, subject to their respective laws and military regulations.

105. The Security Working Group (SWG) is the technical body, comprised of appropriate experts from the Core Mission Partners (CMPs), which supports the security governance process for the CFBLNet on behalf of the C-EG. The terms of reference and responsibilities of the SWG are described within Annex A, Terms of Reference.

Amendments

106. Annex C may be amended when the SWG determines that there is an identified requirement. The SWG Chairman will propose the text of the amendment to the SWG members for endorsement. Once the SWG members have endorsed the amendment, it will be submitted via the document management process as controlled by the Document Working Group (DWG) for C-EG approval. Upon approval by the C-EG, the Secretariat will re-issue a new version of Annex C.

Effective Date

107. The current version of CFBLNet Pub 1, Annex C is effective upon the latest approval by the C-EG.

CHAPTER 2 – SECURITY OF INFORMATION

Infrastructure and Mode of Operation

201. The CFBLNet consists of the following components:

a. Backbone infrastructure (BLACKBONE): A common, closed, **Unclassified** routed IP V4/V6 network layer implemented using a mixture of both serial, ATM and IP bearer networks. Its primary purpose is to transport encrypted traffic throughout the network. The level and type of network services available within this component will be the minimal required to support the interconnection of multiple enclaves as agreed to by all CMPs.

b. CFBLNet Unclassified Enclave (CUE): A permanent routed IP V4/V6 enclave operating over the BLACKBONE and for a period of time over legacy ATM and IP bearer network infrastructures. It will operate at the **Unclassified, Non Releasable to Internet Releasable to CMPs and to Guest Mission Partners (GMPs)** as directed by the C-EG. It must be noted that the CUE can not be connected to any classified domains (though it may support any number of 'dummy' domains).

c. BLUE Enclave: A permanent classified IPv4 routed logical network operating over the BLACKBONE and for a period of time over legacy ATM and IP bearer network infrastructures. **It operates as a System High** logical network at the **SECRET level, releasable AUSCANNZUKUS + NATO**. An agreed level and implementation of Security architecture within this enclave will be determined by the SWG in light of anticipated activities.

d. Temporary Enclaves: An enclave created for a finite period to support the execution of specific Initiatives and operating over the BLACKBONE and for a period of time over legacy ATM and IP bearer network infrastructures. The level of classification and release caveats used within these enclaves will be determined by the Initiative requirements. The coordination and provision of all network services within a specific temporary enclave will be the responsibility of the Initiative sponsor. The CFBLNet SWG has a major advisory role in light of anticipated activities and shall advise on common coalition agreed standards, levels and implementation of security architecture(s) within this enclave.

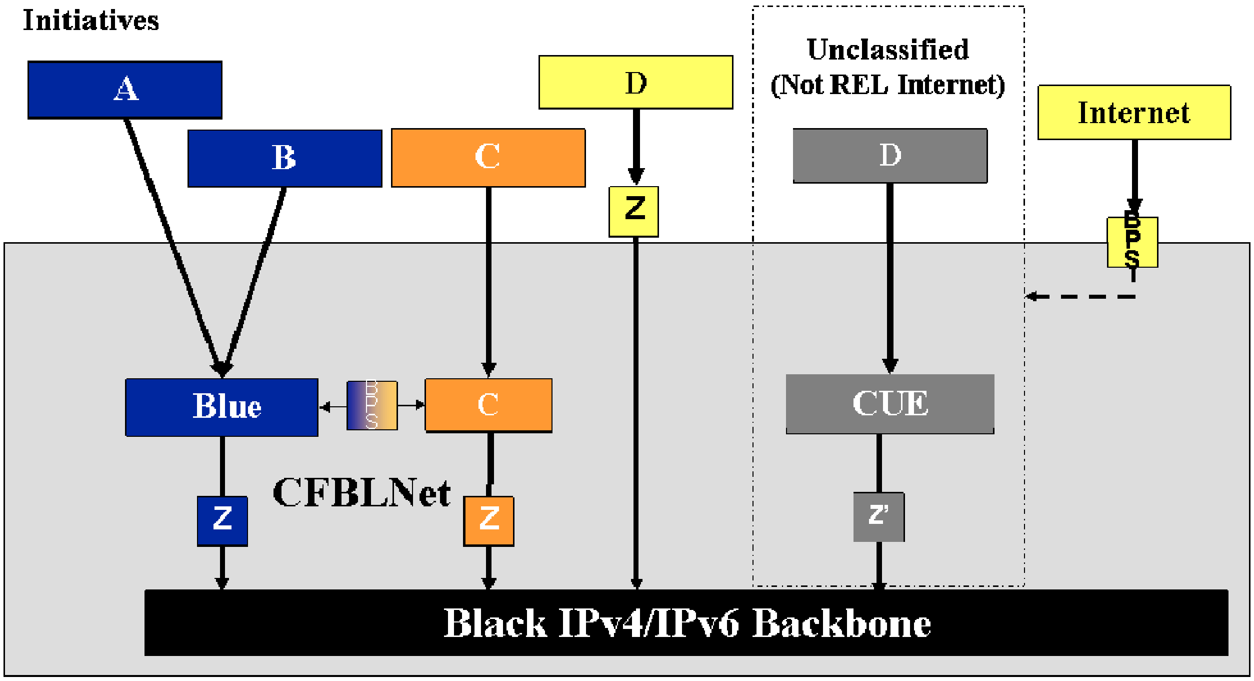

Figure C-1. CFBLNet Architecture Logical view

Cryptographic Separation

202. CFBLNet enclaves are protected by appropriate and approved encryption devices and border protection systems (BPS) accredited by CMPs for the protection, as required, of information up to and including the classification level of SECRET. SECRET Enclaves shall be cryptographically separated from other enclaves by Type 1/NATO-approved products.

Classification of Information

203. CFBLNet enclaves permit handling, forward, storage and transport of information classified up to and including SECRET. CFBLNet data shall be labeled with a releasability caveat determined by the Initiative accreditation, as specified in the CFBLNet Initiative Information Package (CIIP).

204. CFBLNet CMPs and Sponsored Nations/Organisations (GMP) users shall hold an appropriate security clearance valid for the duration of the authorized access and have a need to know. Separation of information domains on the network is achieved through technical and/or procedural means, to enforce the principle of "need to know".

205. Each nation and NATO has their own way of protectively marking information for CFBLNet release. The following are samples of protective marking/security caveats and are equivalent to 'RELEASABLE to AUSCANZUKUS and NATO':

a. Australia: RELEASABLE to AUSCANZUKUS and NATO
b. Canada: RELEASABLE to AUSCANZUKUS and NATO
c. New Zealand: RELEASABLE to AUSCANZUKUS and NATO

d. United Kingdom: RELEASABLE to AUSCANZUKUS and NATO
e. United States: RELEASABLE to AUSCANZUKUS and NATO
f. NATO: NATO UNCLASSIFIED RELEASABLE to AUSCANZUKUS.

206. CFBLNet can use subsets of the above caveats for individual Initiatives as appropriate.

207. Appendix 6 provides guidance on how to classify information related to the conduct of Initiatives on CFBLNet.

Information release between CMPs

208. Release of CFBLNet-related information from one CMP to another CMP falls, by default, under one of the following documents:

a. CFBLNet Technical Arrangement;
b. 5 eyes Memorandum Of Understanding 'CJM3IEM' managed by the CCEB;
c. NATO Security Agreements.

Information release to GMPs

209. A Non-Chartered Nation/Organization can only request sponsorship to participate in an Initiative over the CFBLNet, through a Sponsoring Charter Nation/Organization. The procedure on how to sponsor a non-Chartered Nation/Organization is described in Annex F.

Handling of Commercial Information

210. Commercial and Non-Military agencies/companies who are CMP sponsored to connect must adhere to National/Organizational Military Security and Installation standards. Commercial and Non-Military agencies/companies installation need to be isolated/protected from other networks based on the aforementioned standards.

211. Each nation/organization has a different caveat for protecting commercial information, listed below are examples of the national/organizational caveats for protecting commercially sensitive information. Any information marked with the caveats below shall not be shared with other commercial parties and Initiatives without the written permission of the originating party.

a. Australia – COMMERCIAL-IN-CONFIDENCE
b. Canada – PROTECTED (Commercial in Confidence)
c. New Zealand – COMMERCIAL-IN-CONFIDENCE
d. United Kingdom – COMMERCIAL
e. United States – Unclassified Proprietary
f. NATO – Commercial-in-Confidence

CHAPTER 3 – SECURITY ASPECTS OF NETWORK ARCHITECTURE

Network Architecture

301. Detailed descriptions of the CFBLNet Communications and Information System (CIS) architecture can be obtained from the CFBLNet Pub1, Annex D.

Initiative Architecture

302. The CIIP will contain all the details of the security architecture for a given Initiative (see Chapter 4 on the security aspects of the CIIP). The SWG considers the Initiative proposal based on the most recent version of its CIIP and any other details provided through the CMP Lead Representative (CLR) or Initiative Lead. The CFBLNet SWG is required to advise the C-EG on the security architecture of the proposed Initiative.

303. The CFBLNet SWG will require Initiatives to stand up and maintain an Initiative Chaired Security WG. This selection will be done on a case by case basis depending upon one or more of the following criteria:

a. Multiple domains or enclaves;
b. Cross domain solutions;
c. Multiple classification and/or releasability;
d. Long term initiatives.

Generic Security Requirements

304. Initiative Requirement. The requirement for interconnecting an enclave to another enclave shall be formally stated by the requesting CMP. The Initiative requirement shall identify, as a minimum, the classification of the information to be exchanged.

305. Security Requirement. Prior to implementation of the interconnection, the security requirement shall be established and documented in accordance with the requirements of the CMP Accreditation Authorities.

306. Risk Assessment/Risk Management. The interconnection shall be subject to the requirements of the CMP Accreditation Authorities for risk assessment and risk management; and shall be subject to on-going risk management (The CFBLNet Risk Assessment and Mitigation Strategy described in Appendix 1 should be used as the baseline for this activity) . Where a risk assessment identifies requirements for stronger, or additional, security functions than those stated below, those requirements shall be assessed by the SWG and implemented as required.

307. Security Vulnerability Testing. Security vulnerability testing by the lead CMP for the Initiative is to verify that interface devices, services and procedures are correctly configured and implemented. The security vulnerability testing plan need to be agreed by all CMPs involved in the Initiative.

308. Security Education and Awareness. The Initiative users, system and security administrators shall be provided with on-going security education to maintain a high level of

security awareness of the technical and non-technical security measures in place for the protection of information and inter-networking services and enclave assets.

309. Accreditation. The interconnection shall be accredited (or have an Interim Approval to Operate, IATO) by the appropriate CMP Accreditation Authorities endorsed by the MSAB and approved by the C–EG (see Chapter 5).

310. Disconnection of Service. Site and Initiative security accreditation must remain current or services will be disconnected. It is the CMP Accreditation Authority responsibility to disconnect the CMP site under their responsibility when the sites are no longer accredited.

Interconnection Scenarios

311. The diagram below illustrates the various interconnection scenarios for which Boundary Protection and encryption requirements have been defined by the SWG and endorsed by the MSAB. Initiatives relying on other interconnection scenarios shall refer back to the SWG who will provide further guidance on a case by case basis.

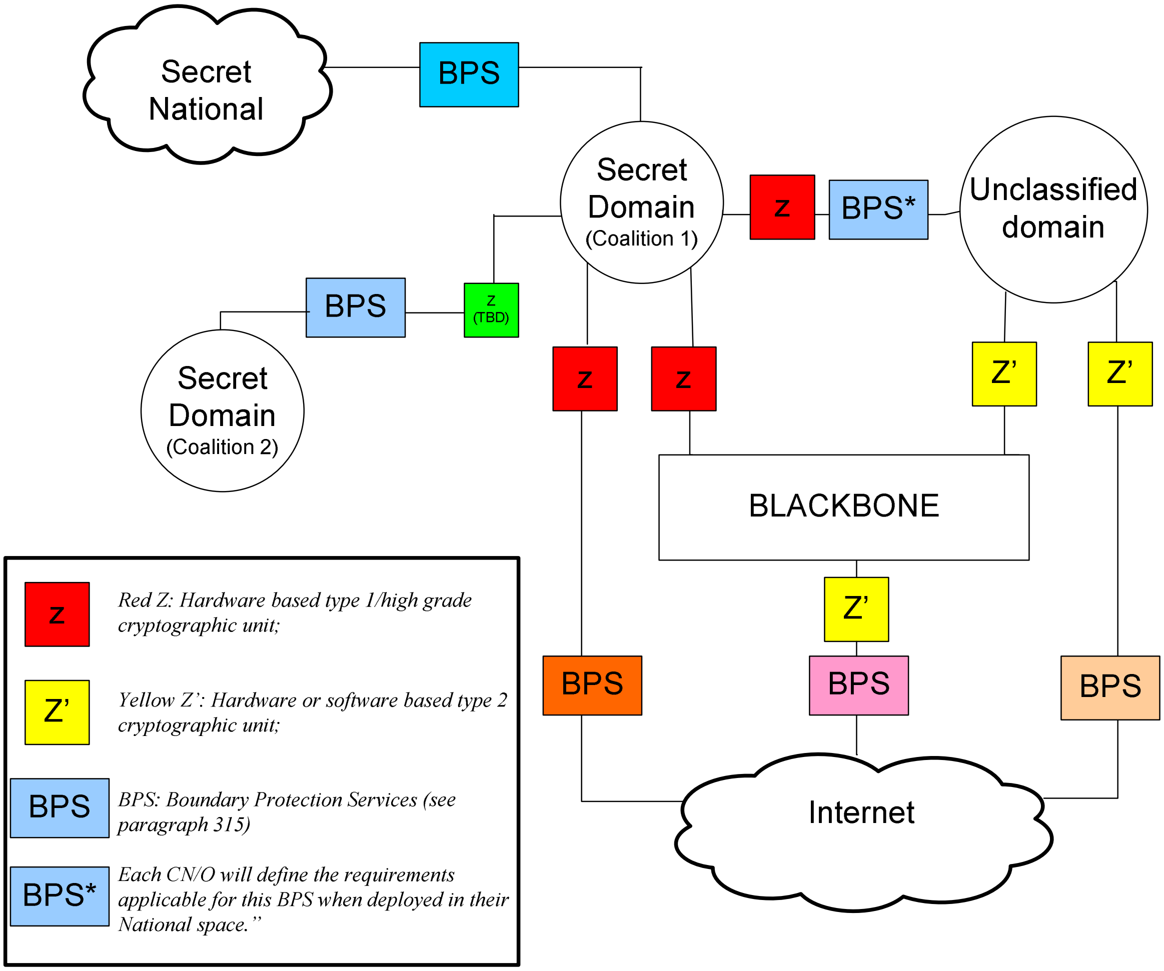
Secret National
BPS
Secret Domain (Coalition 1)
z
BPS*
Unclassified domain
BPS
z (TBD)
Secret Domain (Coalition 2)
z
z
Z'
Z'
BLACKBONE
Z'
BPS
BPS
BPS
Internet
z
Red Z: Hardware based type 1/high grade cryptographic unit;
Z'
Yellow Z': Hardware or software based type 2 cryptographic unit;
BPS
BPS: Boundary Protection Services (see paragraph 315)
BPS*
Each CN/O will define the requirements applicable for this BPS when deployed in their National space."

Figure C.2: Interconnection scenarios for Initiatives running over the CFBLNet

312. Possible interconnections between enclaves are only allowed when permitted by the CFBLNet SWG through the CFBLNet EG. The request is to be forwarded via the SWG to the MSAB for guidance and endorsement.

313. Boundary Protection Services (BPS) is a generic concept that provides security services (through tools, processes and procedures) needed whenever an enclave interfaces with another. These services can be provided by any of a number of tools and devices, such as firewalls, encryption devices, routers, filters, guards, proxy servers, etc., either alone or in combination. The requirements for BPSs are addressed in each interconnection scenario.

314. When GMPs are involved, BPS (if any) must be fully controlled and monitored by the Sponsoring CMP.

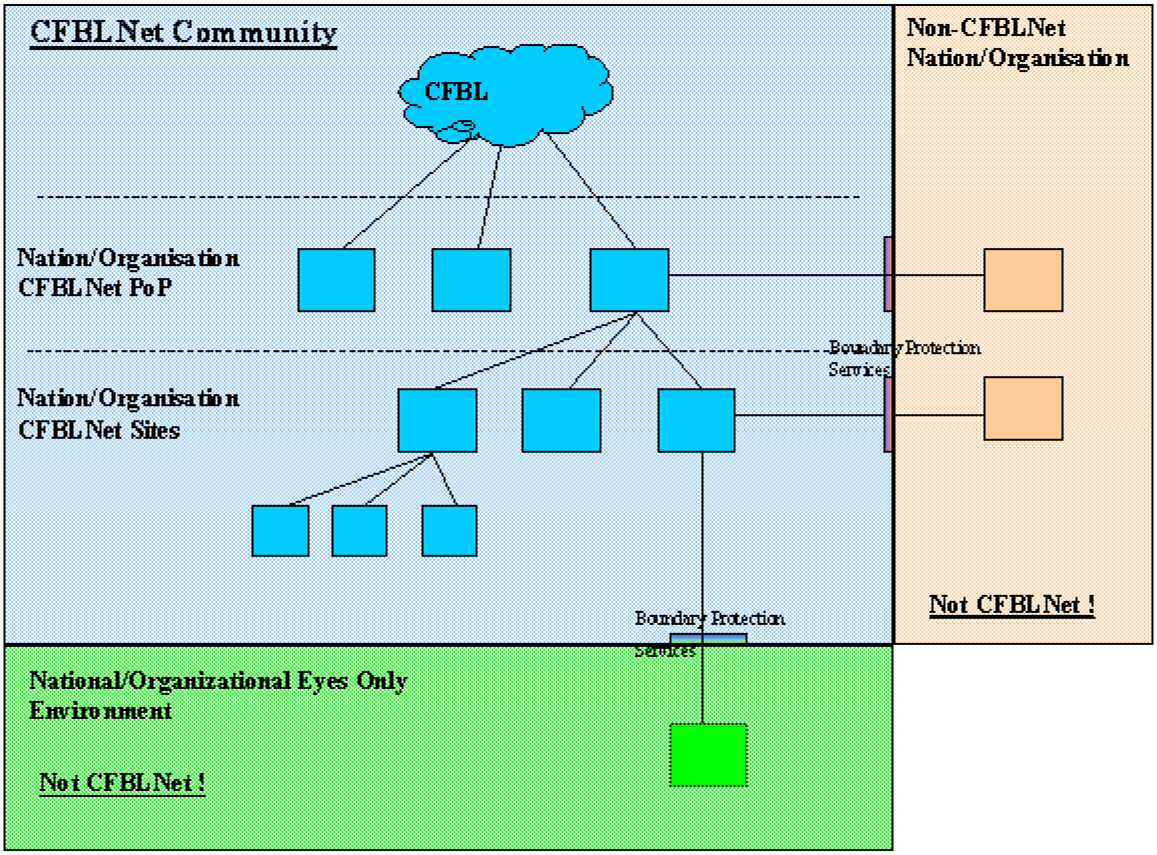
CFBLNet Community
CFBL
Nation/Organisation CFBLNet PoP
Nation/Organisation CFBLNet Sites
Non-CFBLNet Nation/Organisation
Boundary Protection Services
Boundary Protection Services
Not CFBLNet !
National/Organizational Eyes Only Environment
Not CFBLNet !

Figure C.3: CFBLNet and non-CFBLNet communities.

BPS Requirements for Connections to the Internet[1]

315. SECRET network **cannot** be **directly** connected to the internet. However, indirect connection to the Internet can be considered if this connection is compliant with the connecting Nation's policy and all participating Nations of a given Initiative are informed of and endorse this connection.

316. The minimum Boundary Protection Requirements for connecting an UNCLASSIFIED Network to the Internet are:

a. a Common Criteria EAL-2 evaluated (or National equivalent) firewall;
b. an Intrusion Detection System (IDS) tool (desirable though not required for the CUE);
c. a malicious content checker updated at least weekly or on CERT recommendation.

317. The minimum Boundary Protection Requirements for connecting the BLACKBONE to the Internet is:

a. Filtering router with Access Control List (which can not be remotely managed through the Internet).

BPS Requirements for Connections of Domains or Enclaves of Different Releasability

318. Initiatives with a requirement to connect domains or enclaves of different releasability shall refer back to the MSAB Reps of the CMPs involved in this Initiative who will provide further guidance on a case by case basis. The CFBLNet SWG should be fully engaged at the early stages of the discussion and will provide recommendations to the MSAB.

BPS Requirements for Back-End Connections to National Systems

319. The minimum Boundary Protection Requirements for connecting a SECRET Network to a National Secret System are:

a. minimum Common Criteria EAL 4 (or National equivalent) Guard[2]
b. an Intrusion Detection System (IDS) tool;
c. malicious content checker updated at least weekly or on CERT recommendation;
d. a keyword search tool.

[1] The use of the Internet as a transmission path for CFBLNet Communications has been raised with the National Cryptographic Authorities during CMM held in October 2003 and acknowledged.

[2] A classified CFBLNet enclave may be connected to a dummy domain by an unevaluated BPS, controlled by that member CMP. The dummy domain needs to be maintained at the appropriate security protection level for the classification of the information being exchanged.

BPS Requirements for the Connections of Sponsored Nations to the BLACKBONE

320. Sponsoring CMP is required to provide and control a filtering router to the Blackbone or CUE for Sponsored nations that:

a. filters on all protocols;
b. defaults to deny all;
c. only allows point to point IP;
d. locked down to CMP requirements;
e. is not remotely managed.

321. Such filtering router can have multiple GMP on it and does not require any formal evaluation. However, GMP's traffic flow should be isolated from other CMP traffic that is not part of the Initiative.

Encryption/Tunnelling Requirements

322. The Minimum Encryption/Tunneling Requirements for sending Unclassified information from an Unclassified Domain through the Blackbone or the Internet are:

a. a hardware or software based type 2 cryptographic unit (Z') with the following features:
   i. 128 AES or 1024 RSA algorithm;
   ii. US Federal Information Processing Standards (FIPS) 140-2 or Common Criteria EAL2 (or national equivalent) evaluated;
   iii. IPv6 compatible (desirable)

b. cryptographic keys shall be distributed according to an agreed and published key management plan.

323. The Minimum Encryption/Tunneling Requirements for sending Classified information from a Secret Domain through an Unclassified domain, the Blackbone or the Internet are:

a. a hardware based type 1/high grade cryptographic unit (Z) with the following features:
   i. National evaluation and/or approval to use the cryptographic unit to encrypt classified information (up to the required level);
b. cryptographic keys shall be distributed according to national policies and key management plan.

324. Other initiatives with a requirement to send Classified information from a Secret Domain through another Secret Domain but with a different releasability scheme shall refer back to the MSAB Reps of the CMPs involved in this Initiative who will provide further guidance on a case by case basis. The CFBLNet SWG should be fully engaged at the early stages of the discussion and will provide recommendations to the MSAB.

Use of Unevaluated/Unapproved Devices

325. All cross-domain interconnections using unevaluated or unapproved devices require a security risk assessment compliant with International Standards (e.g. ISO,17799, ISO27001, ISO27002, NIST800-30) to be conducted by the sponsor. The following process is to occur:

a. a summary of the risk assessment is to be provided by the appropriate CLR to the Secretariat for distribution to the SWG members to determine the overall risk to the CFBLNet community;
b. the appropriate CMP Accreditation Authority is to provide the risk assessment summary to the appropriate CMP MSAB rep;
c. the CMP MSAB rep provides the risk assessment summary to the MSAB for endorsement; and
d. the recommendations by the SWG and MSAB are to be provided to the CFBLNet Secretariat for the C-EG to evaluate.

CHAPTER 4 – SECURITY ASPECTS OF THE CIIP

Introduction

401. The SWG considers an Initiative proposal based on its published CIIP and any other details provided through the Initiative Briefing. In particular, Tab 6 of the CIIP addresses the security aspects of the Initiative and, for that reason, is a major input for the SWG.

Legal Framework

402. One important thing, often overlooked when filling up Tab 6, is the identification of the Memorandum of Agreement (MOA) or Information Sharing Agreement (ISA) covering the exchange of classified data between all participating CMPs and GMPs in each domain or enclave used by the Initiative. As a matter of fact, the issue of releasability, exploitation and further reuse of classified Initiative data is not covered by the CFBLNet Technical Arrangement and, from a legal point of view, needs to be addressed formally before the Initiative is able to proceed. An MOA/ISA needs to be in place and effective for the complete duration of the Initiative it is covering.

Interconnections

403. The SWG is also expecting Tab 6 to provide the most accurate picture of all the interconnected enclaves and cross domain boundaries to be used by the Initiative. It is highlighted that, in the case of an interconnection of a CFBLNet enclave with a non-CFBLNet enclave, additional threats against the confidentiality, integrity and availability of CFBLNet information and the integrity and availability of the CFBLNet arise because of, for instance:

a. the increased number of users of the enclaves;
b. backend connections that may be unknown to the system/security managers/data owners of the enclaves;
c. connections to the Internet.

404. The SWG will assess the level of risk associated to such interconnections and will take into consideration factors like:

a. the inter-networking services allowed across the interconnection;
b. the Evaluation Assurance Level (EAL) of the security-enforcing components of the CFBLNet enclave Boundary Protection Services (BPS);
c. the operation and maintenance of the interconnection.

Timelines

405. Since some security requirements (such as those derived from Cross-Domain architectures or scenarios involving GMPs) can have a major impact on the Initiative network architecture, Initiative Lead are encouraged to liaise with the SWG as soon as possible in the CIIP drafting process so as to defuse any issue related to security (that could be raised later during the formal CIIP review).

CHAPTER 5 – SECURITY ACCREDITATION

Introduction

501. Accreditation is defined as a formal declaration by a CMP Accreditation Authority that a CIS or network is approved to operate (store, process or transmit information) in a particular security mode at a defined classification level using a prescribed set of safeguards at an acceptable level of risk. Sites must be accredited before they can be considered official CFBLNet Sites. Initiative must also be accredited for a given site in order to use the infrastructure of this site. The following certificates are being used to indicate the accreditation status of Sites and Initiatives:

a. Site-National Accreditation Endorsement Certificate (S-NAEC). This certifies that a site has met the security requirements for a baseline of equipment that is used to transport information between CFBLNet member sites. The time period of a valid S-NAEC is controlled by each CMP Accreditation Authority. All S-NAEC's will be issued by the MSAB. It must be noted that the CUE requires its own accreditation (that cannot exceed the CFBLNet Site Accreditation timeframe).
b. Initiative-National Accreditation Endorsement Certificate (I-NAEC). This certificate in conjunction with an S-NAEC permits a site to participate in a CFBLNet Initiative. The maximum time an I-NEAC is valid for is one year.
c. The above documents will be issued by each nation's respective MSAB rep.

Security Accreditation Authorities

502. The authorities involved in the process for gaining accreditation and authority to operate are:

a. CMP Accreditation Authority
b. MSAB
c. GMP Accreditation Authority (through the sponsoring CMP Accreditation Authority)
d. CFBLNet Secretariat (for record purpose only)

Role of the CMP Accreditation Authority

503. The CMP Accreditation Authority is responsible for the accreditation of all infrastructure and services located behind its CMP boundary or POP and including the GMPs under its responsibility.

504. When a site has achieved CMP accreditation, the CMP Accreditation Authority makes a formal declaration of this to his MSAB representative and requests the site be certified as an official CFBLNet site. This formal declaration takes the form dictated by national or organizational policies.

505. The CMP is also responsible for ensuring that each proposed Initiative has met similar standards for accreditation, and makes a formal representation of such to his MSAB representative. Any and all security issues raised by the MSAB representative must be

satisfactorily addressed by the CMP Accreditation Authority before the MSAB member will further process the site or Initiative request.

Role of the MSAB

506. The MSAB is the security accreditation endorsement authority for activities executing within the CFBLNet CIS.

507. The MSAB Chair coordinates the completed Site or Initiative National Accreditation Endorsement Certificates (S-NAEC or I-NAEC) from the CMP Accreditation Authorities, via the relevant MSAB representative.

508. The MSAB Chair also coordinates the completed Site or Initiative National Accreditation Endorsement Certificates (S-NAEC or I-NAEC) from the GMP Accreditation Authorities, via the sponsoring CMP MSAB representative.

509. A Statement of Conformity (SOC), will be required for each project or initiative by the invited / guest nation's to the appropriate MSAB representative (or MSAB Chair) as formal acknowledgement that an agreed upon formal accreditation process is followed. The initiative or system will be accredited, physically labeled and protected to the level of the appropriate classification of information stored, processed or communicated on that initiative or system.

510. If a specific Initiative utilizing the CFBLNet requires further confirmation of national accreditation status, it will be the responsibility of the Initiative management to solicit the required confirmation from the MSAB.

Role of the Secretariat

511. The Security Coordinator of CFBLNet Secretariat maintains copies of the official MSAB records (NAECs) of all accredited components (Sites, Enclaves and Initiatives) of the CFBLNet.

512. The CFBLNet Secretariat can access an up-to-date copy of the CFBLNet related MSAB records (NAECs) to advise as appropriate the CLR(s) and ensure that there is no lapse in the accreditation of CMP CFBLNet Sites. Any question(s) regarding S and/or I-NEAC(s) should be addressed through the National / Organizational MSAB Rep. The MSAB is the sole authority on National and Organizational Site and Initiative security accreditation matters.

Accreditation Procedures

Overview

513. The accreditation process can be seen as a process parallel but independent of the CIIP approval process (which is described in Annex B of Publication 1). All requirements relating to accreditation, including Core and Guest Mission Partners are addressed in the MSAB accreditation .policy.

514. In summary, Site or Initiative accreditations are first issued by CMP Accreditation Authority, who submits the request and accreditation information to his MSAB representative. When all CMP security requirements have been met, the MSAB member generates a Site National Accreditation Endorsement Certificate (S-NAEC) and/or an Initiative National

Accreditation Endorsement Certificate (I-NAEC), which is submitted to the MSAB Chair, other MSAB members and the Security Coordinator of the Secretariat.

Site Accreditation

515. In order for an Initiative to be conducted, at least two approved involved sites must have their Site and Initiative Accreditations. Other sites will be able to join later on as their Site and Initiative NAECS are endorsed by the MSAB.

516. The Site Accreditation process starts with the CMP Site Security Authority checking the implementation of the security requirements applicable to the connection of the Site infrastructure to the CFBLNet. The CFBLNet Site Interconnection Approval Guidelines at Appendix 2 can be used as guidance when going through this process.

517. When the Site/Local Accreditation Authority has determined that the site has met the specified security requirements, he sends the Site Accreditation package to the CMP Accreditation Authority for approval.

518. When the CMP Accreditation Authority has determined that the Site has been correctly accredited to CMP and CFBLNet standards he submits the accreditation package to the CMP MSAB Representative for Endorsement. The MSAB Rep then determines whether the Site has been accredited in a manner which satisfies CFBLNet requirements.

519. For non-chartered Nations/Organizations the sponsor is responsible for the compliance of the GMP with all applicable security requirements. Details of this compliance are forwarded to the Sponsoring Nation MSAB Member.

520. When the CMP MSAB Rep has endorsed the site accreditation he completes the S-NAEC (see NAEC template at Appendix 5) and notifies the MSAB Chair, the other MSAB members and the Security Coordinator of the Secretariat that the site has approval to operate.

Lapse in the Renewal of S-NAECs

521. If an S-NAEC expires during the conduct of an Initiative, then the Site has to immediately stop its support to this Initiative. However, this does not stop the other involved sites from supporting the same Initiative.

522. It is the responsibility of the CLR to prevent this situation from happening by ensuring that there is no lapse in the renewal of the accreditation of his National/Organizational CFBLNet Site(s).

523. The CFBLNet Secretariat will send the CLR a reminder two months before the expiration of an S-NAEC.

524. Eventually, a warning will be sent by the CFBLNet Secretariat to the CLR eight weeks before the expiration of an S-NAEC.

Initiative Accreditation

525. The Initiative Accreditation process starts with the CMP Security Authority checking the implementation of the security requirements applicable to the connection of the systems

supporting a given Initiative to one or more approved CFBLNet Sites. The CFBLNet Initiative Connection Approval Guidelines at Appendix 3 can be used as guidance when going through this process.

526. When the CMP Accreditation Authority has determined that the Initiative correctly implements the CMP and CFBLNet security standards he submits the accreditation package to the CMP MSAB Representative for Endorsement. The MSAB Rep then determines whether the Initiative has been accredited in a manner which satisfies CFBLNet requirements.

527. When the CMP MSAB Rep has endorsed the Initiative accreditation he completes the I-NAEC (see NAEC template at Appendix 5) and notifies the MSAB Chair, the other MSAB members and the Security Coordinator of the Coalition Project Office Secretariat that the Initiative on that site has approval to operate.

528. The decision on whether an Initiative already accredited requires a new accreditation depends upon the software and hardware configuration / changes that will have occurred since the last accreditation. The decision rests with the Site/Local Accreditation Authority in co-ordination with the Initiative Lead and Lead CMP Accreditation Authority. Where no accreditation is required, the Site/Local Accreditation Authority will notify the Initiative Lead, who will inform the National/Organizational Leads and CFBLNet Secretariat Coordinator.

529. Initiative Accreditation procedures are the same for classified and unclassified enclaves.

Note: In some cases the CMP Accreditation Authorities for Unclassified Initiative is different than for Classified Initiative. This might have an effect on the CMP accreditation timelines.